JOB TITLE: CYBERSECURITY SYSTEMS ENGINEER I [132-45A, 45B, 45C, 45D]

Minimum Experience: 1-5 yrs.

Functional Responsibilities:

- Analyzes user's requirements, concept of operations documents, and high level system architectures to develop network requirements specifications
- Guides users in formulating requirements, advises alternative approaches, and conducts feasibility studies
- Provides technical leadership for the integration of network requirements, design, and technology
- Incorporates new network plans, designs and systems into ongoing operations
- Develops network architecture and network design documentation
- Guides network development and implementation planning through assessment or preparation of network engineering management plans and network integration and test plans
- Designs and performs integration of new technologies into local and wide area networks
- Provides advanced troubleshooting and problem resolution of complex network problems
- Performs administration duties for networking hardware including routers, switches, hubs, gateways, access points, network interface cards, networking cables, network bridges, modems, ISDN adapters, firewalls and other related network hardware
- Interacts with the customer/Government regarding Systems Engineering technical considerations and for associated problems, issues or conflicts
- Provides comprehensive definition of all aspects of system development from analysis of mission needs to verification of system performance
- Performs evaluation of system alternatives and assessment of risks and costs

Minimum Education: BA/BS or Equivalent

JOB TITLE: CYBER PROJECT MANAGER II [132-45A, 45B, 45C, 45D]

Minimum Experience: 5-10 yrs.

Functional Responsibilities:

- Responsible for the successful cost, schedule, performance and quality of the contract
- Serves as the main point of contact for the Contracting Officer (CO), the Contracting Officer's Representative (COR), the Government Program Manager, and the Contractor's senior management
- Ensures proper performance of tasks necessary to ensure the most efficient and effective execution of the contract
- Utilizes expert communication skills needed to direct the skilled technical resources and report on the technical progress, issues, and problem areas, as well as write and review technical documents
- Plans, executes, and finalizes projects that meet or exceed customer objectives
- Develops the overall project plan and manages project operations
- Manages the project stakeholders, project team, project risk, project schedule, project budget, and project conflicts
- Ensures team members know and execute their respective roles and the roles of the other team members
- Ensures proper relationships are established between customers, teaming partners, and vendors to facilitate the delivery of information technology services

Minimum Education: BA/BS or Equivalent

JOB TITLE: CYBER PROJECT MANAGER I [132-45A, 45B, 45C, 45D]

Minimum Experience: 1-5 yrs.

Functional Responsibilities:
- Responsible for the successful cost, schedule, performance and quality of the contract
- Serves as the main point of contact for the Contracting Officer (CO), the Contracting Officer's Representative (COR), the Government Program Manager, and the Contractor's senior management
- Ensures proper performance of tasks necessary to ensure the most efficient and effective execution of the contract
- Utilizes expert communication skills needed to direct the skilled technical resources and report on the technical progress, issues, and problem areas, as well as write and review technical documents
- Plans, executes, and finalizes projects that meet or exceed customer objectives
- Develops the overall project plan and manages project operations
- Manages the project stakeholders, project team, project risk, project schedule, project budget, and project conflicts
- Ensures team members know and execute their respective roles and the roles of the other team members
- Ensures proper relationships are established between customers, teaming partners, and vendors to facilitate the delivery of information technology services

Minimum Education: BA/BS or Equivalent

JOB TITLE: PENETRATION TESTER III [132-45A]

Minimum Experience: 10+ yrs.

Functional Responsibilities:
- Conducts and/or supporting authorized penetration testing on enterprise network assets
- Emulates adversarial cyber activities to identify weaknesses, enumerate vulnerabilities, and assess the overall security posture of customer networks and information systems
- Analyzes site/enterprise DCO policies and configurations and evaluates compliance with regulations and enterprise directives
- Assists with the selection of cost-effective security controls to mitigate risk
- Assesses threats to the environment via penetration testing, risk assessments and other assessments
- Provides inputs on the adequacy of security designs and architectures
- Supports cybersecurity assessments, defensive and offensive operations
- Provides support to security certification test and evaluation of assets, vulnerability management and response, security assessments, and provides customer support and guidance

Minimum Education: BA/BS or Equivalent

JOB TITLE: PENETRATION TESTER II [132-45A]

Minimum Experience: 5-10 yrs.

Functional Responsibilities:
- Conducts and/or supporting authorized penetration testing on enterprise network assets
- Emulates adversarial cyber activities to identify weaknesses, enumerate vulnerabilities, and assess the overall security posture of customer networks and information systems
- Analyzes site/enterprise DCO policies and configurations and evaluates compliance with regulations and enterprise directives
- Assists with the selection of cost-effective security controls to mitigate risk
- Assesses threats to the environment via penetration testing, risk assessments and other assessments
- Provides inputs on the adequacy of security designs and architectures

- Supports cybersecurity assessments, defensive and offensive operations
- Provides support to security certification test and evaluation of assets, vulnerability management and response, security assessments, and provides customer support and guidance

Minimum Education: BA/BS or Equivalent

JOB TITLE: PENETRATION TESTER I [132-45A]

Minimum Experience: 1-5 yrs.

Functional Responsibilities:
- Conducts and/or supporting authorized penetration testing on enterprise network assets
- Emulates adversarial cyber activities to identify weaknesses, enumerate vulnerabilities, and assess the overall security posture of customer networks and information systems
- Analyzes site/enterprise DCO policies and configurations and evaluates compliance with regulations and enterprise directives
- Assists with the selection of cost-effective security controls to mitigate risk
- Assesses threats to the environment via penetration testing, risk assessments and other assessments
- Provides inputs on the adequacy of security designs and architectures
- Supports cybersecurity assessments, defensive and offensive operations
- Provides support to security certification test and evaluation of assets, vulnerability management and response, security assessments, and provides customer support and guidance

Minimum Education: BA/BS or Equivalent

JOB TITLE: INTRUSION/THREAT DETECTION ANALYST III [132-45C]

Minimum Experience: 10+ yrs.

Functional Responsibilities:
- Responsible for intrusion detection, response, investigation, correlation, analysis, and reporting
- Performs command and control functions in response to incidents
- Conducts cyber incident trend analysis and malware analysis
- Tests, implements, deploys, maintains, and administers the infrastructure systems which are required to effectively manage the DCO provider network and resources
- May participate in risk assessment during the Certification and Accreditation process

Minimum Education: BA/BS or Equivalent

JOB TITLE: INTRUSION/THREAT DETECTION ANALYST II [132-45C]

Minimum Experience: 5-10 yrs.

Functional Responsibilities:
- Responsible for intrusion detection, response, investigation, correlation, analysis, and reporting
- Performs command and control functions in response to incidents
- Conducts cyber incident trend analysis and malware analysis
- Tests, implements, deploys, maintains, and administers the infrastructure systems which are required to effectively manage the DCO provider network and resources
- May participate in risk assessment during the Certification and Accreditation process

Minimum Education: BA/BS or Equivalent

JOB TITLE: INTRUSION/THREAT DETECTION ANALYST I [132-45C]

Minimum Experience: 1-5 yrs.

Functional Responsibilities:
- Responsible for intrusion detection, response, investigation, correlation, analysis, and reporting
- Performs command and control functions in response to incidents
- Conducts cyber incident trend analysis and malware analysis
- Tests, implements, deploys, maintains, and administers the infrastructure systems which are required to effectively manage the DCO provider network and resources
- May participate in risk assessment during the Certification and Accreditation process

Minimum Education: BA/BS or Equivalent

JOB TITLE: RISK/VULNERABILITY ANALYST II [132-45D]

Minimum Experience: 5-10 yrs.

Functional Responsibilities:
- Performs data gathering, research, and analysis while conducting threat, vulnerability, risk, and maturity assessments
- May apply critical thinking, conduct gap analysis, and develop implementation plans for the improvement of the risk management-related program
- Contributes to constant innovation and improvement

Minimum Education: BA/BS or Equivalent

JOB TITLE: RISK/VULNERABILITY ANALYST I [132-45D]

Minimum Experience: 1-5 yrs.

Functional Responsibilities:
- Performs data gathering, research, and analysis while conducting threat, vulnerability, risk, and maturity assessments
- May apply critical thinking, conduct gap analysis, and develop implementation plans for the improvement of the risk management-related program
- Contributes to constant innovation and improvement

Minimum Education: BA/BS or Equivalent

JOB TITLE: CYBER SECURITY/RISK AUDITOR III [132-45D]

Minimum Experience: 10+ yrs.

Functional Responsibilities:
- Assists in evaluating cyber security risks, testing controls designed to mitigate risk, communicating issues and findings to management
- Devises solutions for business improvements, and follows-up on corrective actions
- May participate on to execute technical audit projects focused on evaluating the effectiveness of cyber security governance, tools and operations
- May evaluate the design, effectiveness and efficiency of information technology and security processes, procedures, and technical controls including solution implementations, identify and address systemic gaps in cyber security risk management

Minimum Education: BA/BS or Equivalent

JOB TITLE: CYBER SECURITY/RISK AUDITOR II [132-45D]

Minimum Experience: 5-10 yrs.

Functional Responsibilities:

- Assists in evaluating cyber security risks, testing controls designed to mitigate risk, communicating issues and findings to management
- Devises solutions for business improvements, and follows-up on corrective actions
- May participate on to execute technical audit projects focused on evaluating the effectiveness of cyber security governance, tools and operations
- May evaluate the design, effectiveness and efficiency of information technology and security processes, procedures, and technical controls including solution implementations, identify and address systemic gaps in cyber security risk management

Minimum Education: BA/BS or Equivalent

JOB TITLE: CYBER SECURITY/RISK AUDITOR I [132-45D]

Minimum Experience: 1-5 yrs.

Functional Responsibilities:

- Assists in evaluating cyber security risks, testing controls designed to mitigate risk, communicating issues and findings to management
- Devises solutions for business improvements, and follows-up on corrective actions
- May participate on to execute technical audit projects focused on evaluating the effectiveness of cyber security governance, tools and operations
- May evaluate the design, effectiveness and efficiency of information technology and security processes, procedures, and technical controls including solution implementations, identify and address systemic gaps in cyber security risk management

Minimum Education: BA/BS or Equivalent

GSA PRICES FOR HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

ITEM	LABOR CATEGORY	YEAR 4 9/1/17 - 8/31/18	YEAR 5 9/1/18 - 8/31/19
001	Cybersecurity SME II	$157.57	$162.30
002	Cybersecurity SME I	$124.15	$127.87
003	Information Assurance/Cybersecurity Analyst II	$138.47	$142.62
004	Information Assurance/Cybersecurity Analyst I	$105.05	$108.20
005	Cybersecurity Software Developer III	$157.57	$162.30
006	Cybersecurity Software Developer II	$128.93	$132.80
007	Cybersecurity Software Developer I	$109.82	$113.11
008	Cybersecurity Systems Engineer III	$148.03	$152.47
009	Cybersecurity Systems Engineer II	$128.93	$132.80
010	Cybersecurity Systems Engineer I	$ 80.22	$82.63
011	Cyber Project Manager II	$143.25	$147.55
012	Cyber Project Manager I	$105.05	$108.20
013	Penetration Tester III	$167.13	$172.14
014	Penetration Tester II	$124.15	$127.87
015	Penetration Tester I	$ 95.50	$98.37
016	Intrusion/Threat Detection Analyst III	$152.80	$157.38
017	Intrusion/Threat Detection Analyst II	$114.60	$118.04
018	Intrusion/Threat Detection Analyst I	$ 95.50	$98.37
019	Risk/Vulnerability Analyst II	$143.25	$147.55
020	Risk/Vulnerability Analyst I	$124.15	$127.87
021	Cyber Security/Risk Auditor III	$167.13	$172.14
022	Cyber Security/Risk Auditor II	$148.02	$152.46
023	Cyber Security/Risk Auditor I	$105.05	$108.20